

[RENESAS SECURITY PROCESS INTRODUCTION TRAINING]

# OUTLINE OF CYBERSECURITY MANAGEMENT SYSTEM FOR AUTOMOTIVE PRODUCTS

REV.3.0 3RD JUN. 2024 REL/QAD/QSP/QDSC S. NAGATA, K. AMIMOTO, K. FUJII



© 2024 Renesas Electronics Corporation. All rights reserved.

RENESAS CONFIDENTIAL

RENESAS

This video is a lecture video that provides an outline of the cybersecurity management system for automotive products.



## TRAINING REQUIREMENT PER ROLE

◎:Mandatory  
○:Recommendation  
-:Option

Training Module		A	B	C	D
Role	Role definition	Security Management System Outline (0.5h)	Product Development Process (2h)	Security Incident Vulnerability Treatment (1h)	Security Asset Management (1h)
Security Leader	TOS-DS00216	◎	◎	◎	◎
Security Assessor	LLWEB-20100376	◎	◎	◎	◎
Technical Reviewer	TOS-DS00214	◎	◎	◎	◎
PSIRT member	AST-BD-21-0042	○	—	○	—
Product design engineer		○	○	○	○
Person related to factory		○	—	—	○

© 2024 Renesas Electronics Corporation. All rights reserved.

RENESAS CONFIDENTIAL

Page 2

RENESAS

This is a table of participants for each training module.

We offer four training modules as security process introduction education.

The main roles in security-enabled development are security leaders, security assessors, technical reviewers, and PSIRT.

This table shows the training required for each role.

Double circles are mandatory, circles are recommendation, and bars are option.

Role definition have been established for each role, setting out certification and appointment procedures. It specifies the training required for certification.

This course, Security Management System Outline, is considered essential education for certification of security leaders, security assessors, and technical reviewers.



## INTRODUCTION OF EACH TRAINING MODULE

Training Module	A Security Management System Outline (0.5h)	B Product development Process (2h)	C Security Incident Vulnerability treatment (1h)	D Security Asset management (1h)
In-house standards (technical standard)	–	TOS-DS00146 RCT-JB2019/5007	RCT-JF3009 TOS-DS00196	RCT-JB0026 RCT-JB0027
International Standard etc.	–	IEC 62443-4-1, ISO 21434	IEC 62443-4-1, ISO 21434	IEC 62443-4-1, ISO 21434
Training Content	<ol style="list-style-type: none"><li>1. Necessity for cyber security (15 min.)</li><li>2. Our main security process (15 min.)</li><li>3. Summary (1 min.)</li></ol>	<ol style="list-style-type: none"><li>1. Outline (10 min.)</li><li>2. Requirement management process (30 min.)</li><li>3. Semiconductor product development (20 min.)</li><li>4. Software product development (30 min.)</li><li>5. Management process (30 min.)</li><li>6. Contract with customer / supplier selection (5 min.)</li><li>7. Summary (3 min.)</li></ol>	<ol style="list-style-type: none"><li>1. Outline (10 min.)</li><li>2. Corrective action when incident occur (30 min.)</li><li>3. Continuous improvement activity (20 min.)</li><li>4. Summary (3 min.)</li></ol>	<ol style="list-style-type: none"><li>1. Necessity of security asset management (20 min.)</li><li>2. Classification and management methods of security property (20 min.)</li><li>3. Procedure of security asset management (10 min.)</li><li>4. Summary (3 min.)</li></ol>

An introduction of each training module.

It shows related in-house standards, international standards, and the content of each training.

This course provides an outline of security management systems and is considered an introductory course.

Before taking the B, C and D education, you can take this course to get an overall picture and then move on to the specifics, so that you can proceed with your studies smoothly.

The total length is 30 minutes.



## PURPOSE OF THIS COURSE

- Understand the necessity for cybersecurity.
- Understand outline of the cybersecurity process and cybersecurity management system.

This is the purpose of this course.  
One is to understand the necessity for cybersecurity.  
And understand the outline of the cybersecurity process and  
cybersecurity management system.



## CONTENT

---

- 1. Necessity for cybersecurity**
- 2. Our main security processes**
- 3. Summary**

This is the content of this course.  
First, the necessity for cybersecurity.  
Second, our main security processes.  
Third, summary.

# 1. NECESSITY FOR CYBERSECURITY



First, the necessity for cybersecurity.



## EXAMPLE OF SECURITY BREACH (AUTOMOTIVE)



### Security defect in Tesla Model S keyless in 2018.

The security research team of a Belgium university succeeded in being able the release of the lock by invading key fob with the owner and the communication with the car from the Tesla car under parking with the radio signal stolen with a tool related to the wireless, reading the encryption rule built into key fob, deciphering, not driving for two seconds, and stealing the code.  
(quoted from WIRED Mobility 2019.09.24 TUE 15:30)

### Jeep Cherokee hacking in 2015

It has been understood to be operated remotely from the outside by hacking in spite of while running when two specialists of the computer security of the United States do the safety experiment of "Jeep Cherokee" made of Fiat Chrysler Automobiles (FCA).  
(quoted from Sankei news 2015.8.2)



Here's an example of a car security breach.

The two cases listed here did not actually cause any damage.

This is an example of a researcher reporting that a car's system has a vulnerability that can be hacked.

Let's start with the matter above. The Tesla case uses a vulnerability in the keyless entry system. A demo video shows how to hack the car. Electronically copy the owner's key, use it to unlock the door, then start the engine and drive away. Tesla is offering rewards to people who report issues. Tesla reportedly paid the research team at the University of Belgium \$10,000, or about 1.1 million yen, as a reward. Tesla is immediately modifying its keyless entry system to address this vulnerability. However, even after fixing this 2018 issue, keyless systems are still being broken by this research team.

This is an example that shows that cybersecurity measures are a cat-and-mouse game.

As for the Jeep issue below, 1.4 million units were recalled. The experts who hacked this chip have published a white paper reporting how they did it.

According to the document, it was stated that the firmware of Renesas' V850/FJ3 had been rewritten so that commands could be sent via CAN bus. By being able to send commands via CAN bus, you will be able to freely control all components in your car, including the steering wheel, engine, transmission, and braking system. If the steering wheel suddenly turns while driving, it could lead to a serious accident. It's scary just thinking about it.

As I will explain on a later page, cybersecurity measures for automobiles have become mandatory. Not only OEM companies, but as seen in the Jeep example, there is a possibility that our products could be misused, so we must take this seriously.



## EXAMPLE OF SECURITY CASE (INDUSTRIAL CONTROL SYSTEM)



### Power failure with Ukraine malware in 2016

The cyber attack to the electric power company generated in Ukraine (Kiev) came for the command (breaker interception) not intended with the malware to be transmitted, and for the power failure of 1 hour or less and 15 minutes to occur in a region concerned on December 17, 2016. (Quoted from "Cyber, incident case 2 related to the regulating system" of IPA. )

### Shutdown with ransomware of semiconductor plant (TSMC) in 2018

The damage of ransomware WannaCry was received and it influenced a lot of computers and the manufacturing devices. Thing that amount of damage by stoppage in production of three days reaches 19 billion yen or less with operating profit base (Quoted from "Cyber, incident case 6 related to the regulating system" of IPA. )



Next, I will introduce security incidents related to industrial systems. These were actually attacked. The example shown here is an example of a control system security breach. Control systems that are separate from internal information systems are also under attack. Cyber attacks on information systems are often reported in the news. In November 2020, it was reported that Mitsubishi Electric suffered a cyberattack and information such as the addresses and bank accounts of business partners was leaked to an external party. Cyberattacks thus occur on a daily basis.



## CYBER ATTACK

Attacker:	Intelligence officer, industrial spy, hacker group, and malicious criminal/person, etc.
Purpose of attack:	Strategic changes of organization bodies such as the criminal for pleasure one, nations, and enterprises, lowering reputations, industrial spyings, and social political insistences, etc. ..money.. stealing
Stage of attack:	<p>Example: Stage of target type attack</p> <p>(1) Plan (<b>attack target setting and relation investigation</b>)</p> <p>(2) Attack preparation (target type mail, website falsification, and C&amp;C server preparation)</p> <p>(3) Initial infiltration (sending of target type mail)</p> <p>(4) Basic construction (backing door establishment, terminal information obtaining, and composition information obtaining)</p> <p>(5) Internal entry and investigation (invasion at the other end and server invasion and manager information theft)</p> <p>(6) Target accomplishment (information theft and crash)</p> <p>(7) Re-invasion (Invade again through the backing door).</p>

Understanding attacker's purpose, and  
forecasting the target aimed at easily beforehand

**It is important as security countermeasures.**



Let's talk about cyber attacks.

This table shows the attacker, the purpose of the attack, and the stages of the attack.

The targeted attacks mentioned here are attacks that attack network devices such as PCs and system computers through networks such as the Internet, causing damage and stealing stored information.

Targeted emails are sent during the initial infiltration stage of No. 3 of this targeted attack. On the other hand, if you educate employees in advance not to open suspicious emails, you can prevent the initial infiltration of No. 3 and end targeted attacks before they occur.

However, if a person with low security awareness opens the email and accesses the link, initial infiltration will be allowed, a malicious program will be executed, and information will be extracted without the user's knowledge. It is necessary to carry out thorough education for this purpose. In this way, it is important to know the purpose of the attack, the likely targets, and the stages of the attack and take countermeasures.



## WHAT IS THE CYBER SECURITY?

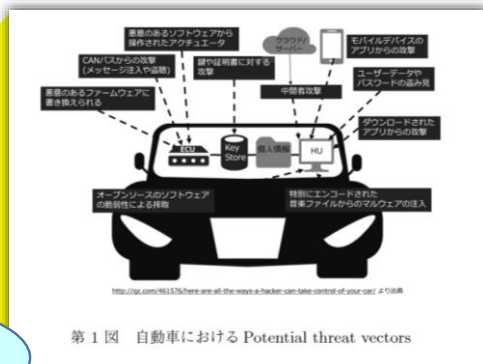
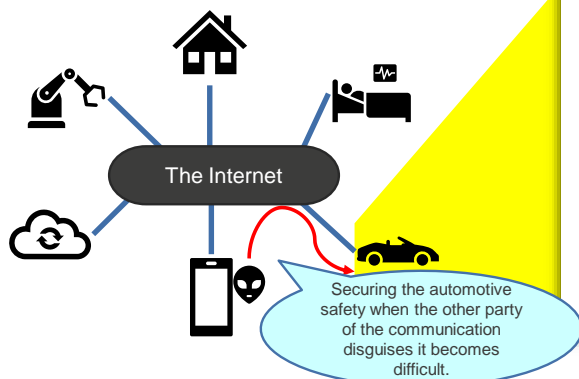
- Give measures to protect data, the system, and the communication route, etc. , and exclude or ease the dangers of the attack and the falsification, etc. from the secret leak and the outside.
- Only it plans once and it doesn't end.  
After the product is shipped according to the environmental transformation and the attacker's evolution, it is necessary to continue measures by the software update etc.

Cybersecurity is defined as taking measures to protect data, systems, communication routes, etc., and eliminating or mitigating risks such as leakage of confidential information, external attacks, and falsification. In short, cybersecurity is about taking measures on your computer and on the Internet to prevent attacks.

For example, in the case of a defect in a semiconductor product, it is possible to correct the circuit, change the material, or take other measures to prevent the defect from occurring again.

On the other hand, the difficult thing about cybersecurity is that just because you have taken countermeasures once, it does not mean that you will never be attacked again. Attackers are also honing their techniques and developing various attack methods. You must always take measures against this, such as updating your software.

## THE CONNECTED WORLD



Source: "Control system security threat and measures" feature title  
From the case in the threat car to the regulating system"

Various threats that connect equipment and service on network and can cause it  
The risk and damage of which it causes them are based beforehand, and it is necessary to  
design and to develop.

A connected world.

Why do cars also require cyber security?

A generation ago, cars didn't need cybersecurity. That's because cars were mechanical. It had nothing to do with computers or the internet. There was no keyless system, so I inserted the key, opened the door, and started the engine. Such mechanical parts are being replaced by electronic devices.

As things become more computerized, such as autonomous driving, and become connected to the Internet, cyber security will become necessary. As shown in this picture, for example, by connecting to smartphones, it becomes necessary to build cybersecurity that assumes attacks from smartphones. Indeed, by becoming more connected, various threats will increase.

## WEAKNESS OF SUPPLY CHAIN

### 【4位】サプライチェーンの弱点を悪用した攻撃 ～業務委託先にも適切なセキュリティ管理を要求～

IPA



- 原材料や部品の調達、製造、在庫管理、物流、販売、業務委託先などの一連の商流(サプライチェーン)において、セキュリティ対策が甘い組織が攻撃の足がかりとして狙われる
- 一部業務を委託している外部委託先組織から情報が漏えい

Copyright © 2020 独立行政法人情報処理推進機構

28

Source: „Ten information security large threats 2020 chapter of the organization (independent administrative agency information processing promotion mechanism (IPA))”

© 2024 Renesas Electronics Corporation. All rights reserved.

RENESAS CONFIDENTIAL

Page 12

RENESAS

Where of the supply chain does the attacker aim?

Here and there, the measures level of the enterprise has the important information that becomes "Money (Kane)" even if it is asunder.

The attacker aims at a low organization of the defense level.



Our company who is the supplier of the semiconductor product

It is a market demand to demand the security management from the IP vender not only its company but also the manufacturing factory and outsourcing ahead.

## Weakness of supply chain.

The automotive industry has a pyramid-structured supply chain with OEM at the top, and tier one and tier two. For example, even if OEM is conscious of cyber security and manages product information well, if the security awareness of Tier 2, which shares the same information for product development, is low, information may be leaked.

As shown in this illustration of the bucket, if the walls are too low, water will leak through them, so if even one organization has low security awareness, information will leak. All walls should be the same height.

There was news that Toyota's factory was shut down due to a cyber attack. It was not Toyota that was attacked, but Toyota's suppliers. It is not known whether they targeted Toyota's suppliers in order to force them to shut down operations. However, as a result, the factory was suspended for an entire day. Not only our company but also our suppliers need to take measures against cyber attacks.



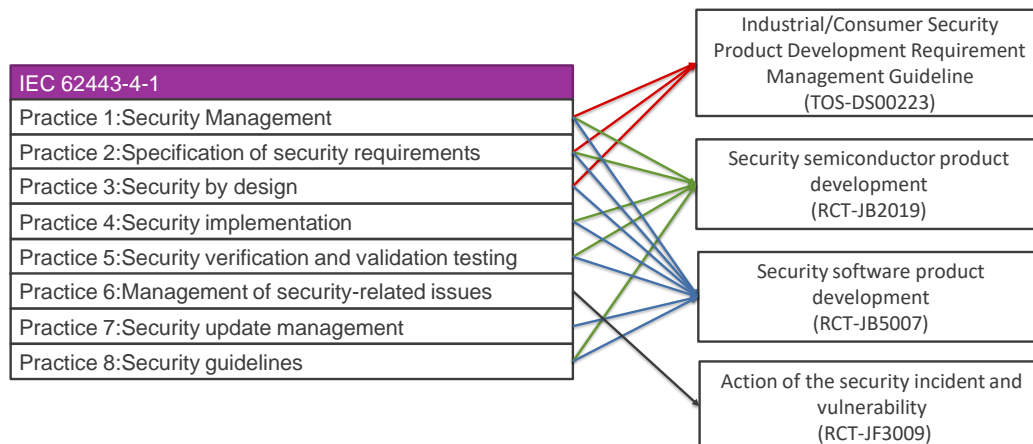
## INTERNATIONAL STANDARD FOR SECURITY PRODUCT DEVELOPMENT PROCESS

■ For industrial equipment	IEC 62443	Established in 2018 (Part4)
■ For automotive	ISO 21434	Establish in 2021

International standard for security product development processes. In this way, cybersecurity has become a natural trend throughout the world. In response to this, international standards have also been established. Regarding cybersecurity for industrial control systems, IEC 62443 was enacted, and ISO 21434 was established in August 2021 regarding automobile cybersecurity. Our company must also comply with these international standards.



## MAPPING OF REQUIREMENT FOR IEC 62443-4-1



Mapping of IEC 62443-4-1 requirements.

The requirements of IEC 62443, the security standard for industrial control systems, have been implemented into our internal processes. Our processes cover requirements ranging from Practice 1 Security Management to Practice 8 Security Guidelines.

The process has been audited by TÜV Rheinland and compliance has been confirmed.

However, since there was no product development to obtain IEC 62443 product certification after process certification, the process certification has now expired.

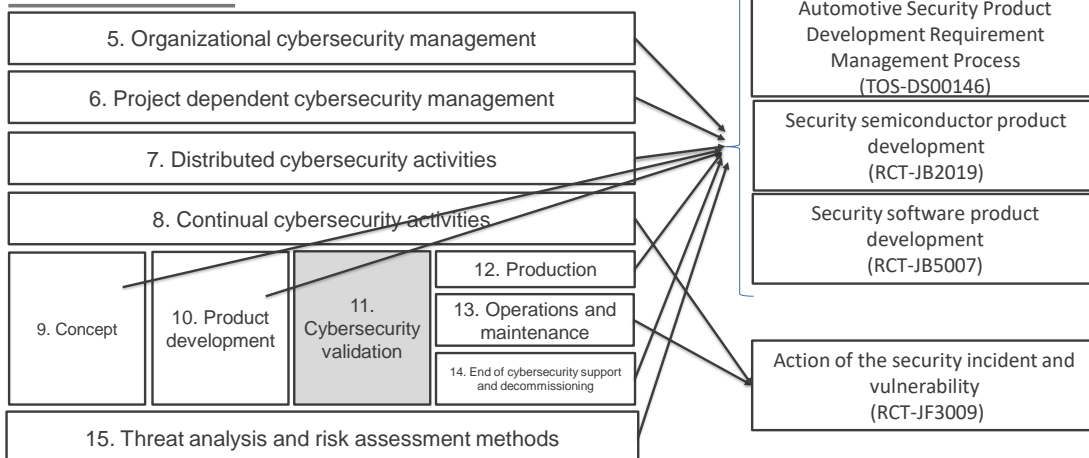
IEC 62443-4-1 was the base process when Renesas' security product development process was built from scratch.

After that, we added the specific requirements of ISO 21434, the automotive cybersecurity standard, to create a product development process for both HPC and EP.

The following is a mapping of its ISO 21434 requirements.



## MAPPING OF REQUIREMENT FOR ISO 21434



※Chapter 11 is out of scope, because they are requirements for item level.

© 2024 Renesas Electronics Corporation. All rights reserved.

RENESAS CONFIDENTIAL

Page 15

RENESAS

We have also completed implementing the requirements of ISO 21434 into our internal processes.

Chapter 11 is not applicable as it is an item level requirement, but other requirements can be covered by our process.

The process has been audited by TÜV Rheinland and compliance has been confirmed.

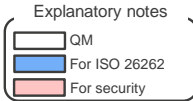
Regarding automotive, a United Nations regulation requiring cybersecurity measures for vehicles will be issued in May 2022. This United Nations regulation requires vehicle manufacturers to obtain ISO 21434 process certification, and vehicle manufacturers also require their suppliers to take cybersecurity measures. When it comes to in-vehicle products, if they don't support cybersecurity, customer won't buy them.

So far, we have explained that cyber-attacks are actually occurring, that automobiles can also be targeted by cyber-attacks, that the entire supply chain needs to address them, that international standards have been established, and that there are I hope that you have understood that cybersecurity measures are necessary in our product development.

## 2. OUR MAIN SECURITY PROCESSES



Cyber security has become essential.  
There may be some of you who would like to know what you should  
do in your product development work.  
In Chapter 2, I will provide an overview of our internal processes for  
cybersecurity.



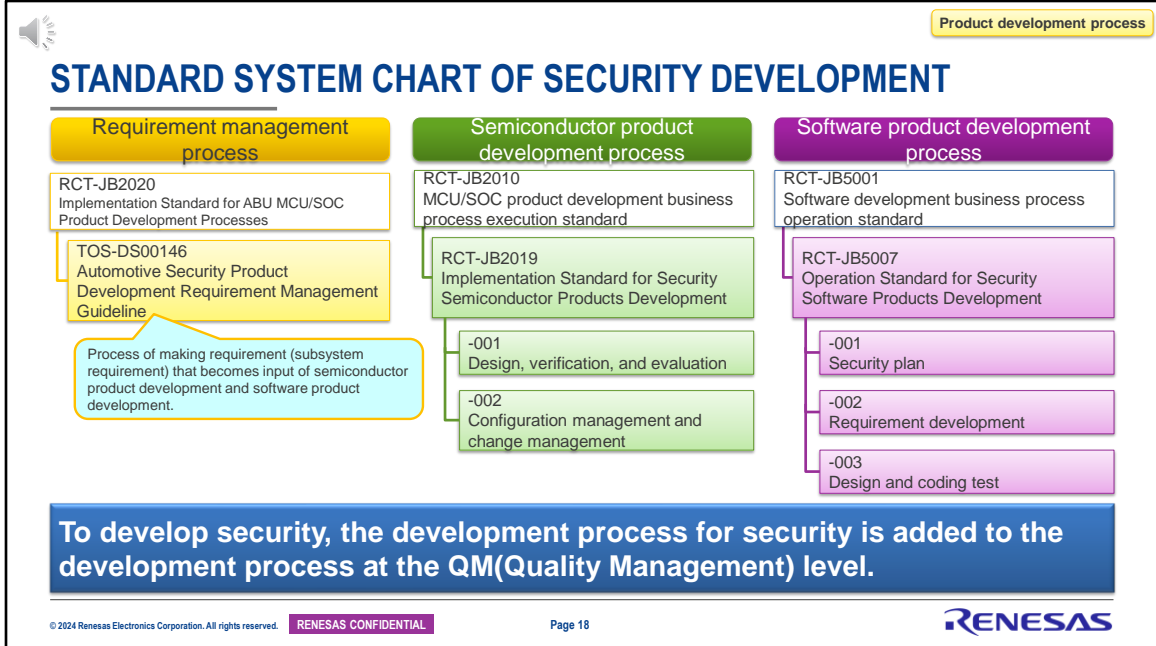
\*1): CC attestation goods

RENESES CONFIDENTIAL

Page 17



17



Standard system chart of security development.

Here we show the standards system for the requirements management process, semiconductor product development process, and software product development process.

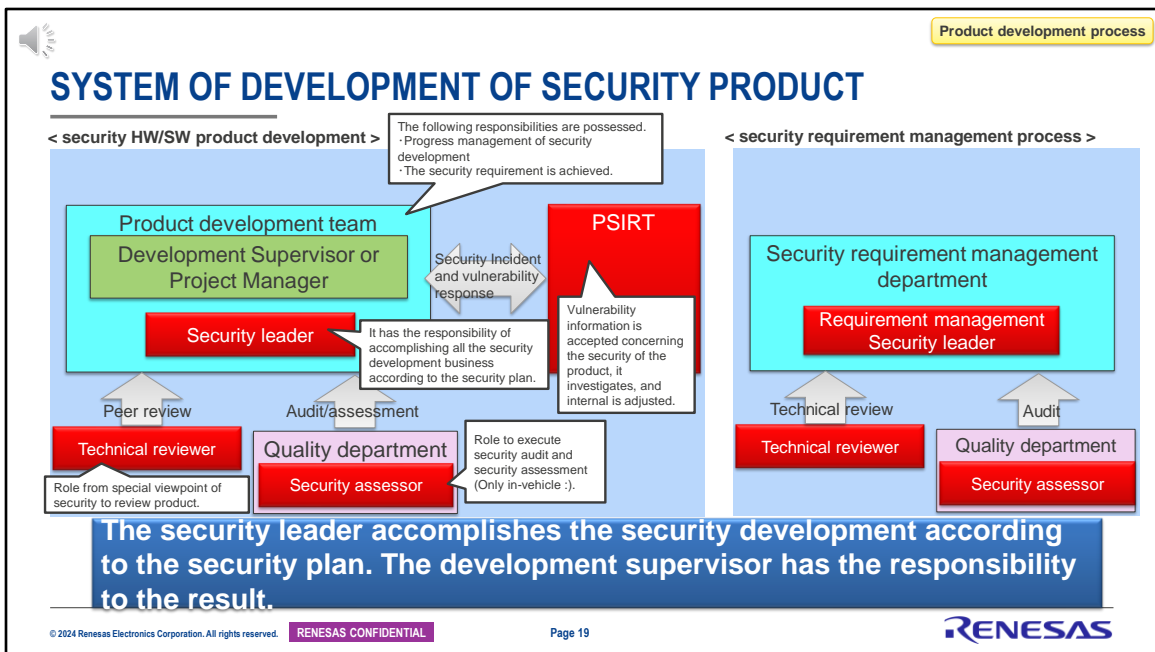
Requirements management will be developed based on RCT-JB2020.

Then, we perform security activities such as threat analysis and security requirement derivation in accordance with TOS-DS00146.

Semiconductor products will be developed based on RCT-JB2010. On top of that, we will conduct security activities such as vulnerability analysis and security evaluation in accordance with RCT-JB2019.

Similarly, software products are developed based on RCT-JB5001. On top of that, we perform security activities such as vulnerability analysis and secure coding in accordance with RCT-JB5007.

All QM level development processes plus security activities are to be implemented.



System of development of security product.

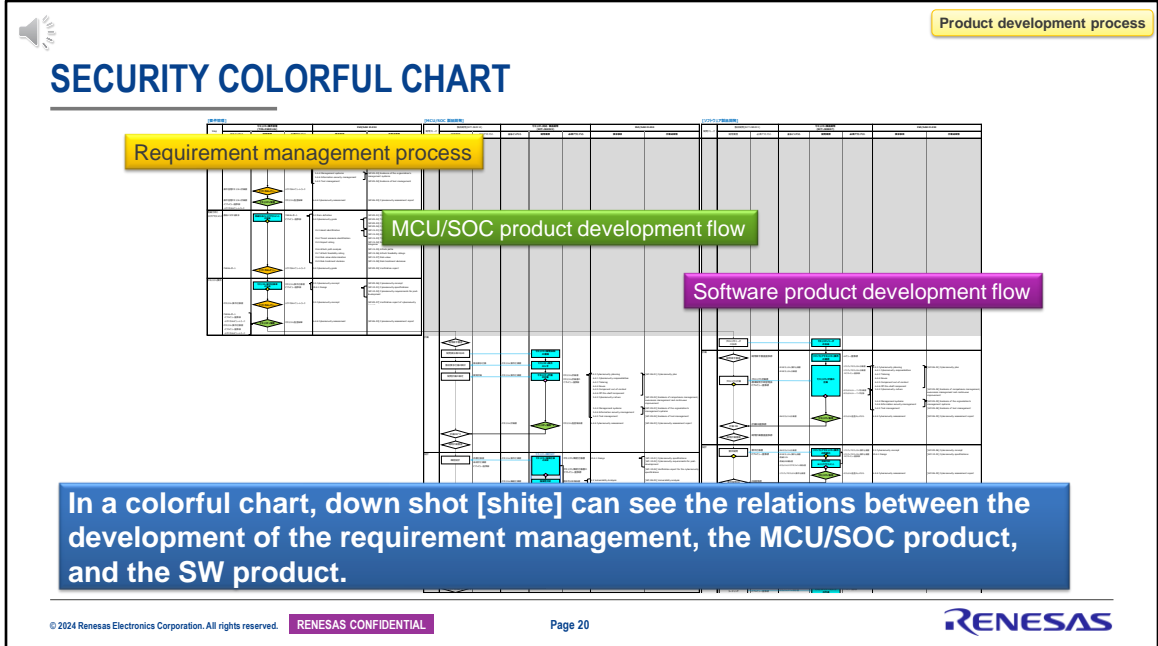
This shows a schematic diagram of the security product development system. The red squares indicate roles specific to security development.

The security leader is responsible for implementing security activities in accordance with the security plan. Security assessors conduct audits and assessments.

Technical reviewers conduct reviews from the standpoint of security experts.

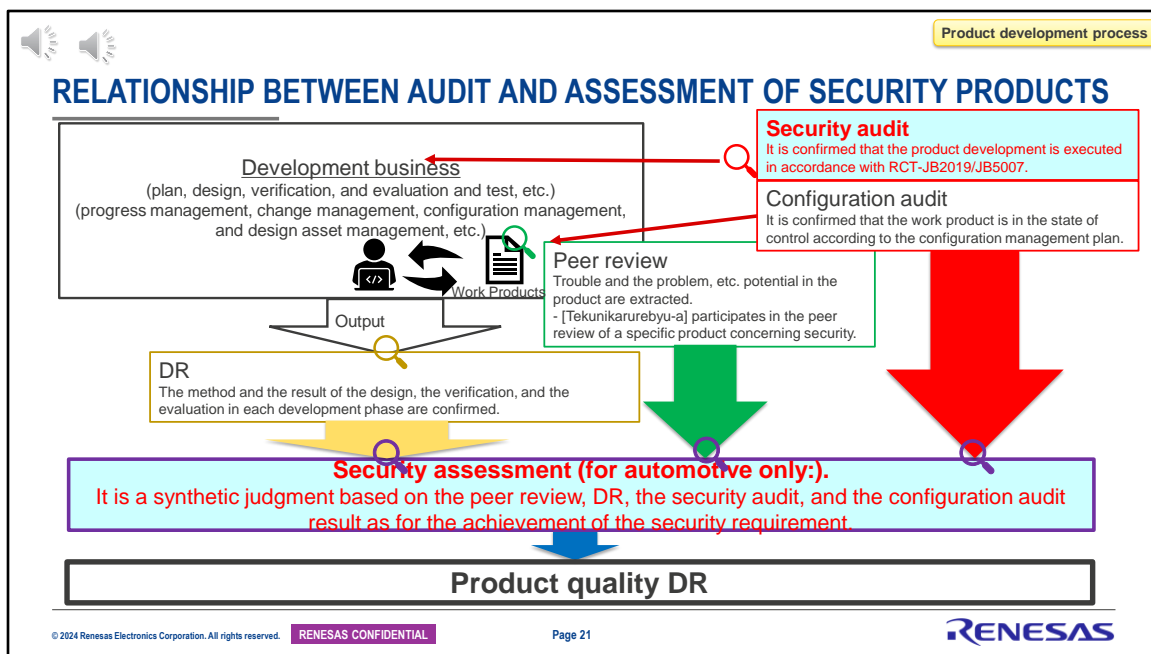
Although we may not be involved much during product development, when a security problem occurs, a team called PSIRT works together to resolve the problem.

Please note that even for security development, the responsibility for product development remains with the development supervisor or project manager.



Security colorful chart. Similar chart are being created for functional safety.

We create a security colorful chart to visualize the security development process. It allows you to visually understand the development flow, process, corresponding ISO 21434 requirements, work products, etc., so please use it as support material when understanding the development process. It has been released as Attachment 1 of TOS-DS00157.



Relationship between audit and assessment of security products. This section briefly explains the relationship between auditing and assessment of security products. Security audits and security assessments shown in red will be added. Ensure that security activities conducted by security leaders follow security development processes such as RCT-JB2019 and RCT-JB5007.

A security audit is to confirm that this has been carried out. What is shown in green is peer review. In the case of security, technical reviewer who are security experts may participate in specific peer reviews that specialize in security. As you already know, DR is a place where related departments participate and confirm the results of development. Security assessments are made based on the results of security audits, peer reviews, and DR. A security assessor conducts security audits and security assessments. The results of the security assessment are one of the items checked during the product quality DR.

Up to this point, I have provided a brief explanation over four pages

starting from page 18. The security product development process is explained in more detail in the training module B.



## SECURITY ASSET MANAGEMENT

There is taking CIA an English initial of three following, too.

(source: ISO/IEC 27000)

- **Confidentiality:** Ensure that only those who are authorized to access the information can access it.
- **Integrity:** Ensuring that the information has not been destroyed, tampered with or erased.
- **Availability:** Ensuring that those who are authorized to access information can access information and related assets without interruption when necessary.



Three elements of information security

**Technological standard to have provided administrative procedure to maintain this CIA**

**Development: “Operation standard for Security Asset Management” (RCT-JB0026)**

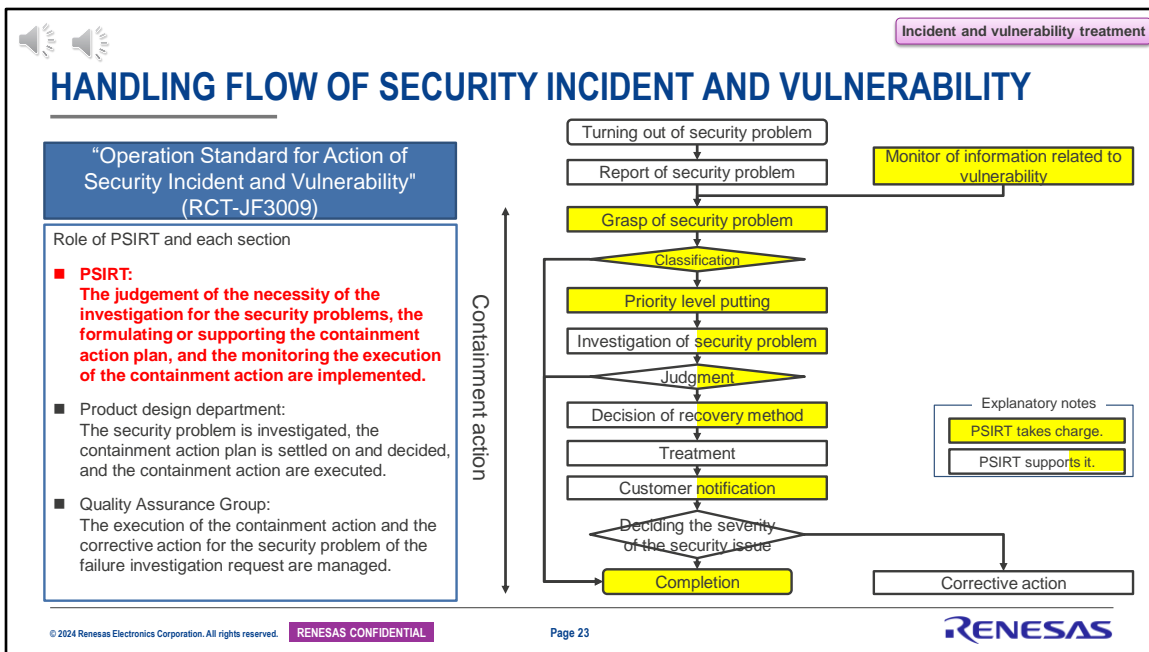
**Manufacturing: “Operation standard for Security Asset Management for REL manufacturing site” (RCT-JB0027)**

Security asset management.

The three elements of information security are confidentiality, integrity, and availability.

Even if a product is equipped with cybersecurity features, if a hacker obtains the design information, it is like having a strategy guide for a game and can be easily exploited. Therefore, information related to security functions must be managed in a way that prevents it from being lost, stolen, rewritten, or discarded. At this time, while maintaining confidentiality and integrity, it would be a problem if the information could not be used when needed, so it is necessary to manage it while also taking availability into account.

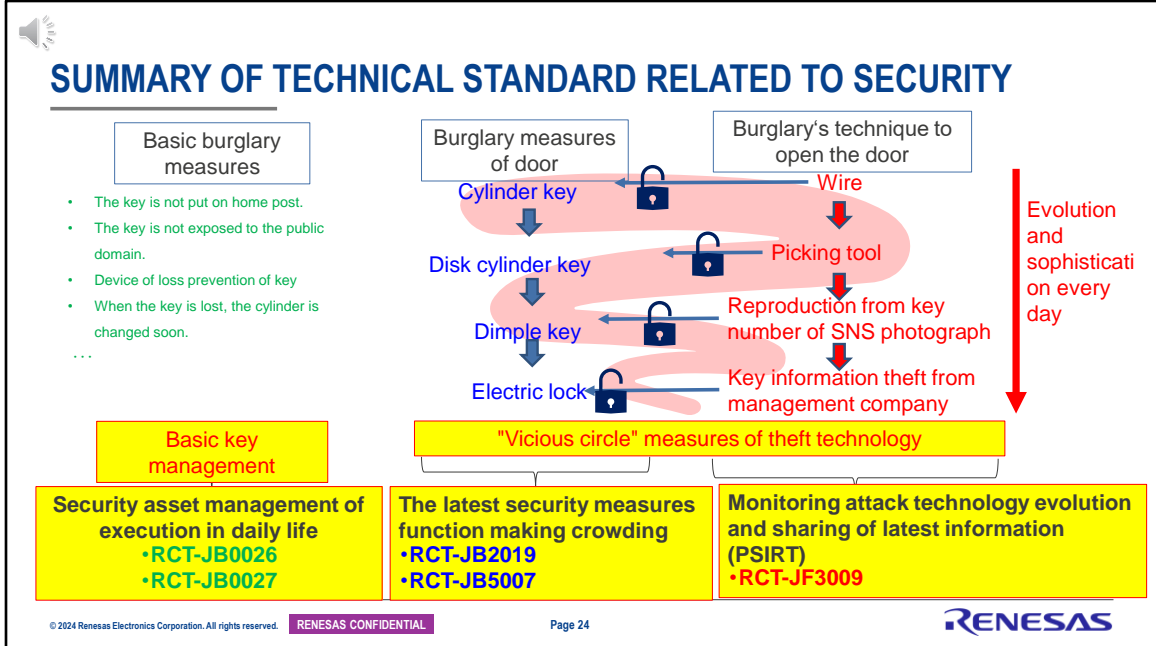
This security asset management will be explained in more detail in the training module D.



Handling flow of Security incident and vulnerability.

Regarding product defect management, QAD performs defect management as the management department. Regarding security, PSIRT, product security incident response team, monitors the implementation of containment actions for security issues. Currently, we are launching PSIRT for HPC and EP. Furthermore, PSIRT work together while sharing necessary information. In addition to conducting emergency activities related to the occurrence of this security issue, PSIRT regularly access public institutions that publish vulnerability information, obtain information that may be related to our company, and provide necessary information. PSIRT also carry out monitoring activities for vulnerability-related information that are distributed internally.

Training module C provides a more detailed explanation of how to deal with the security incident and vulnerability.



## Summary of technical standard related to security.

I have summarized the internal security response process using the example of a burglary. Burglary's techniques to open the door are constantly evolving from wires to key information theft, while door locks are also evolving from cylinder keys to electric locks to prevent them from being broken. While it is important to improve your door lock technology, it is also important to have basic security awareness, such as not leaving your keys in your home mailbox or under a flowerpot. The same goes for cybersecurity measures. In order to respond to the fact that hackers and other attackers are creating new attack methods and improving their technology every day, we are conducting research on the security features of our products, including the advancement of encryption methods.

Of course, it is important to upgrade security measures, but it is also important to manage information security on a daily basis to ensure confidentiality and integrity so that such technical information does not leak.

Security asset management, building security countermeasure functions, and monitoring attack techniques and sharing the latest

information. Please keep in mind that cybersecurity measures are carried out using these three pillars.



## "CYBERSECURITY" SITE

date of issue	title / タイトル
2024/6/11	Updated five technical specifications and added one technical specification in Cybersecurity page.
2024/5/29	Updated "QD 21434-Operations' Subline for Cybersecurity/Interface Agreements and Report" (QD-020758) in Cybersecurity page.
2024/5/19	Issued E-mails for "QD-020712" - 15 form.
2024/5/19	Updated "Procedures of the process compliance check with security" (QD-020714) in Cybersecurity page.

<https://renesasgroup.sharepoint.com/sites/REL-QSP-DQIPortal/SitePages/CyberSecurity.aspx>

Lastly, I would like to introduce a cybersecurity site. Technical standards, technical operating specifications, templates, etc. used in security development are all posted on the Design Quality Information Portal. We also have links to PSIRT pages and training materials.

Please use all means.



### 3.SUMMARY



Finally, a summary.



## SUMMARY

- ◆ Correspondence to cyber security is a natural demand of the market, and it is indispensable to develop and to produce done products for security as our company.
- ◆ It is necessary to do the product development business process, the security asset management, and the security production for security to protect the product from the cyber attack.  
Still, when the security incident and the vulnerability occur, necessary treatment is done according to the correction process of the security incident and the vulnerability.

Responding to cyber security is a natural demand of the market, and it is essential for our company to develop and produce products that are security compatible.

Especially in the security field, cybersecurity measures are mandatory, so there is no loophole.

Second, to protect products from cyber-attacks, we must develop and manufacture the security product in accordance with the security development processes, security asset management, and security production. However, if a security incident or vulnerability occurs, we will follow the security incident and vulnerability handling process and take the necessary actions.

I mentioned this in comparison to the example of a burglary, but in particular security asset management, building security countermeasures, monitoring attack techniques, and sharing the latest information. Please keep in mind that cybersecurity measures are handled through these three pillars.

Thank you for watching till the end.

Ver.	Date	Approval/making	Content
1.0	2020/11/30	Nagata/ Amimoto and Fujii	New making
1.1	2020/12/18	Nagata/ Amimoto and Fujii	Correction of erratum omission of a word etc.
1.2	2021/01/21	Nagata/Fujii	P2,3 Training modules are changed from five to four.
2.0	2022/3/2	Nagata/Fujii	Address for 3 <sup>rd</sup> rev. of TOS- DS00146.
3.0	2024/6/3	Nagata/Fujii	Address for 1 <sup>st</sup> rev. of TOS- DS00223 for EP.



Thank you